COOLEY LLP
MICHAEL G. RHODES (116127) (rhodesmg@cooley.com)
KYLE C. WONG (224021) (kwong@cooley.com)
AARTI G. REDDY (274889) (areddy@cooley.com)
101 California Street, 5th Floor
San Francisco, CA 94111-5800
Telephone: (415) 693-2000
Facsimile: (415) 693-2222

CHARLES A. WOOD (310702) (cwood@cooley.com)
1299 Pennsylvania Ave., NW, Suite 700
Washington, DC 20004
Telephone: (202) 842-7800
Facsimile: (202) 842-7899

Attorneys for Defendant
NOOM, INC.

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

AUDRA GRAHAM and STACY MOISE, individually and on behalf of all others similarly situated,

Plaintiff,

v.

NOOM, INC. and FULLSTORY, INC.,

Defendant.

Case No. 3:20-cv-06903-LB

DEFENDANT NOOM, INC.'S MOTION TO DISMISS PLAINTIFF'S COMPLAINT

Hearing Date: February 18, 2021
Hearing Time: 9:30 a.m.
Judge: Judge Laurel Beeler

NOTICE OF MOTION AND MOTION TO DISMISS

PLEASE TAKE NOTICE that on February 18, 2021, at 9:30 a.m., or as soon thereafter as the motion may be heard in Courtroom B, 15th Floor of the San Francisco Courthouse, located at 450 Golden Gate Avenue, San Francisco, CA 94102, pursuant to Federal Rules of Civil Procedure 12(b)(1) and 12(b)(6), defendant Noom, Inc. ("Noom") will and hereby does move to dismiss the causes of action in plaintiffs Audra Graham and Stacy Moise's ("Plaintiffs") Class Action Complaint filed on October 2, 2020 (ECF No. 1) ("Complaint"). This motion is based on this Notice of Motion and Motion, the accompanying Memorandum of Points and Authorities, the Declaration of Aarti Reddy, the pleadings on file in this matter, oral argument of counsel, and such other materials and argument as may be presented in connection with the hearing of the motion.

STATEMENT OF RELIEF SOUGHT

Noom respectfully seeks an order dismissing the Complaint's causes of action with prejudice for lack of subject matter jurisdiction and failure to state a claim upon which relief can be granted.

STATEMENT OF ISSUES TO BE DECIDED

1. Whether Plaintiffs' claims shall be dismissed for lack of subject matter jurisdiction pursuant to Federal Rule of Civil Procedure 12(b)(1).

2. Whether Plaintiffs state a claim under the California Invasion of Privacy Act ("CIPA"), California Penal Code Sections 631 and 635.

3. Whether Plaintiffs state a claim under the California Constitution for Invasion of Privacy.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page

Cases

TABLE OF CONTENTS

Page

TABLE OF CONTENTS

Page

TABLE OF CONTENTS

Page

Statutes

I. INTRODUCTION

Over the last several years, Plaintiffs' counsel has pursued a meritless campaign to criminalize various companies' routine monitoring of website usage information that those companies use to improve their websites' function and users' experience. This same Plaintiffs' counsel has filed copycat actions in New York, New Jersey and California—each time alleging claims under the Federal or California Wiretap Act ("CIPA"), or other state analogues. So far, the only case in this Circuit that has ever made it past the pleadings stage is both distinguishable and lacking in substantive analysis of the applicable law. Hoping to turn the tides of years of adverse precedent, Plaintiffs' counsel seek to use this decision—and a recent, inapposite opinion from the Ninth Circuit—to push the boundaries of CIPA case law and litigate over a dozen copycat actions currently filed across California.

This case is one such action. Plaintiffs allege that they visited the Noom website on November 17, 2019 and June 23, 2020, respectively, during which times the website purportedly contained code created by FullStory, Inc. ("FullStory") to collect communications between them and Noom's website. (Class Action Complaint, ECF No. 1 ("Complaint" or "Compl.") ¶¶ 4, 5.) Importantly, they do not allege any specific instance of this conduct affecting them, much less that they suffered any harm from the challenged conduct. To the contrary, Plaintiffs concede that this tool was simply used to improve Noom's website design and customer experience—the very experience that Plaintiffs sought when visiting the website. Nonetheless, they claim this practice amounts to Noom "wiretapping" its own communications within the meaning of CIPA, that Noom's possession of the code used to implement this tool also violates CIPA, and that the practice constitutes an invasion of privacy so offensive as to violate the California Constitution.

Notably, the conduct that Plaintiffs seek to criminalize would encompass an extraordinary volume of routine communications that take place many times every second for almost every website on the Internet. It simply cannot be that a website operator or its agent collecting routine browsing information for purposes of improving its website functioning is akin to a surreptitious party listening in on a telephone call. Rather, this conduct is strikingly similar to that of a brick-and-mortar store that might hire a safety consultant to monitor in-store videos of customers to

determine where it could safely put in-store displays, or a theft detection expert to assess cash register activity. To hold otherwise would drastically expand the scope of liability under CIPA, expose vast swaths of website operators to criminal liability, and cause serious repercussions for the basic functionality of the Internet.

It is therefore unsurprising that Plaintiffs' recycled claims suffer from the same fatal defects as those in so many of the cases their counsel has previously filed. As to their wiretapping claims, Plaintiffs fail to explain how a party can eavesdrop on its own communications or aid and abet wiretapping liability merely by giving another party access to its own communications. Plaintiffs' allegations that FullStory intercepted their communications "in transit," are conclusory at best and the claim should be dismissed for this independent reason. Equally deficient are Plaintiffs' allegations that Noom's mere possession of FullStory's code was itself a violation of the wiretap law. They do not allege any injury from Noom's alleged possession of the code, and nowhere do they contend, as they must, that this code was *exclusively* designed as a wiretap. As to their privacy claims, while Plaintiffs spend considerable time describing the hypothetical ills of FullStory's technology, they fail to plead a legally protected privacy interest or reasonable expectation of privacy, much less meet the high bar for violations of the California Constitution.

Consequently, for the reasons discussed below, the Complaint should be dismissed with prejudice in its entirety.

II. BACKGROUND AND PROCEDURAL HISTORY.

Plaintiffs Audra Graham ("Graham") and Stacy Moise ("Moise") allege that they are California residents, though fail to plead where they are domiciled. (Compl. ¶¶ 4, 5.) Each Plaintiff further claims to have "visited" and "browsed" Noom's website (www.noom.com) at least once, and maintain that the site "recorded" their "keystrokes, mouse clicks, and other electronic communications." (*Id.* ¶¶ 1, 2, 4, 5.)

Defendant Noom, Inc. ("Noom"), is headquartered in New York, New York and operates a mobile application that has helped millions of users lose weight and lead healthier lives through behavioral change. (*Id.* ¶ 1.) Users can register for Noom through its website and access its weight loss program through Noom's mobile application.

Plaintiffs allege that Defendant FullStory is a "marketing software-as-a-service [] company" that uses technology to provide online retailers with "marketing data." (*Id.* ¶ 11.) Plaintiffs further allege that Noom "partners" with FullStory and uses its "Session Replay" technology on its website. (*Id.* ¶¶ 31, 12.) According to Plaintiffs, Noom "voluntarily embedd[ed] FullStory software code" on the Noom website "pursuant to an agreement" with FullStory. (*Id.* ¶ 34.)

The Complaint contains remarkably few details describing the technology as implemented by Noom. Instead, Plaintiffs generically allege that Defendants "recorded Plaintiffs' electronic communications in real time, [and] used the intercepted data to attempt to learn their e-mail, height, weight, age range, gender, medical conditions, and other PII and PHI." (*Id.* ¶ 2.) Notably, although Plaintiffs contend that that the code intercepts communications in "real time," they do not explain how the code is deployed or specifically allege that it was triggered simultaneously or before Noom's webpage is loaded. (*Id.* ¶¶ 2, 25-27.) Indeed, Plaintiffs contradict their own "real time" allegations by *also* pleading that the alleged recording in fact occurs "in near real time." (*Id.* ¶ 27.)

Most of Plaintiffs' remaining allegations are a simple copy-and-paste job that mirrors the allegations pled by the same Plaintiffs' counsel in various other copycat actions against FullStory. Plaintiffs' failure to tailor the Complaint to Noom are best evidenced by their description of how FullStory's "Session Replay" technology purportedly operates on a hypothetical website; they offer no allegations describing how *Noom* has actually implemented that technology and used it to collect and transmit Plaintiffs' information to FullStory—key facts that might support, or by their absence refute, their claims. Rather, Plaintiffs plead only conclusory allegations that "Noom knows that FullStory's software captures the keystrokes, mouse clicks and other communications of visitors," that it "pays FullStory to supply that information" and that "upon information and belief, the Session Replay feature in FullStory's software created a video capturing each of Plaintiffs' keystrokes and mouseclicks on the website.[1] (*Id.* ¶¶ 32, 34, 38.)

[1] Plaintiffs also falsely allege that the Privacy Policy on Noom's website fails to account for services such as FullStory's. (*Id.* ¶ 48.) That policy, dated prior to when either Plaintiff visited Noom's website, states that Noom may use "programming code that is designed to collect information about User's interactions with the Website, Mobile App and Services, such as the links User clicks on." Noom Privacy Policy, https://web.noom.com/terms-and-conditions-of-use/noom-privacy-policy/ (last visited December 8, 2020).

Further, while Plaintiffs claim that Defendants "used the intercepted data to attempt to learn" about visitors to Noom's website, (*id.* ¶ 2), they fail to allege that Noom had access to any personally identifiable information ("PII") allegedly collected by FullStory, let alone that this information was ever linked to an identifiable individual or assembled in any fashion. Likewise, Plaintiffs also do not allege that any PII was ever used for marketing or targeting purposes, or that the information collected was ever sold or shared. Instead, they concede that any alleged monitoring was used to help "improve [Noom's] website design and customer experience." (*Id.* ¶ 17.) Accordingly, even if such data were collected or assembled in some fashion, it would not be *personally* identifiable information, as there are no allegations that any information was linked to an identifiable individual.

III. LEGAL STANDARD

Plaintiffs invoke the Class Action Fairness Act ("CAFA") to justify bringing their California state law claims in federal court. (Compl. ¶ 13.) To plead diversity jurisdiction under CAFA, a plaintiff must allege, at a minimum, that at least one plaintiff and one defendant are citizens of different states; that the class contains no fewer than 100 members; and that the aggregate amount in controversy exceeds $5,000,000.00, exclusive of interests and costs. 28 U.S.C. §§ 1332(d)(2), (d)(5). Failure to plead any of these elements mandates dismissal. *Ibarra v. Manheim Investments, Inc.*, 775 F.3d 1193, 1197 (9th Cir. 2015).

Further, Rule 12(b)(6) provides for dismissal of an action for "failure to state a claim upon which relief can be granted." *See* Fed. R. Civ. P. 12(b)(6). For a 12(b)(6) motion, "all well-pleaded allegations of material fact [are accepted as true] and construe[d] in the light most favorable to the non-moving party." *Padilla v. Yoo*, 678 F.3d 748, 757 (9th Cir. 2012). "[C]onclusory allegations of law and unwarranted inferences" are insufficient. *Associated Gen. Contractors v. Metro. Water Dist.*, 159 F.3d 1178, 1181 (9th Cir. 1998) (citing *Pareto v. FDIC*, 139 F.3d 696, 699 (9th Cir. 1998)). A complaint must state "evidentiary facts which, if true, will prove [the claim]," *Kendall v. Visa U.S.A., Inc.*, 518 F.3d 1042, 1047 (9th Cir. 2008), otherwise it will be dismissed. *See Watson v. Weeks*, 436 F.3d 1152, 1157 (9th Cir. 2006).

IV. THE COURT LACKS SUBJECT MATTER JURISDICTION BECAUSE PLAINTIFFS' ALLEGATIONS OF DOMICILE ARE DEFICIENT.

Plaintiffs premise the Court's jurisdiction in this case solely under CAFA, which requires them to plead, among other things, the state in which they are domiciled (i.e., their citizenship). 28 U.S.C. § 1332(d)(2)(A); *see, e.g.*, *Broadway Grill, Inc. v. Visa Inc.*, 856 F.3d 1274, 1275–76 (9th Cir. 2017). Persons are domiciled in the places they reside with the intent to remain or to which they intend to return, *see Kanter v. Warner-Lambert Co.*, 265 F.3d 853, 857 (9th Cir. 2001), but residence is not necessarily the same as domicile. *Id.* ("A person residing in a given state is not necessarily domiciled there, and thus is not necessarily a citizen of that state."). Instead of properly alleging domicile, Plaintiffs each claim that they are "a California resident who lives in [] California." (Compl. ¶¶ 4, 5.) As such, they have not met CAFA's requirements and the Complaint must be dismissed.

Plaintiffs' counsel is well aware of this requirement. Indeed, the Central District of California recently dismissed *sua sponte* a nearly identical suit they brought against FullStory on this very basis. In dismissing the action, the Court observed that "the complaint fails to adequately show the parties are completely diverse" and gave the plaintiff there one week to cure the defect (which Plaintiffs' counsel did not do). *See* Minute Order, *Saleh v. Hudson's Bay Co.*, No. 20-cv-9095 (C.D. Cal. Oct. 8, 2020); Judgment, *Saleh v. Hudson's Bay Co.*, No. 20-cv-9095 (C.D. Cal. Oct. 19, 2020) (citation omitted). The same result follows here: Plaintiffs have not adequately alleged that at least one plaintiff and one defendant are citizens of different states, and the Complaint must therefore be dismissed.[2]

V. THE COMPLAINT FAILS TO STATE A CLAIM.

A. Plaintiffs Fail to State a Claim Under CIPA.

Plaintiffs fail to state a claim under either Sections 631 or 635 of CIPA for the following

[2] Defense counsel contacted Plaintiffs' counsel on November 30 and December 1, 2020 to inform them of this pleading deficiency, but Plaintiffs' counsel refused to amend the Complaint, even after Defense counsel agreed to stipulate to an additional amendment as of right. (Reddy Decl. ¶ 2-4.) Noom believes that Plaintiffs' counsel refusal is motivated by their desire to preview Noom's merits arguments while avoiding an adverse ruling on those issues before further amending their Complaint. As such, Noom requests that the Court dismiss Plaintiffs' complaint on *both* 12(b)(1) and 12(b)(6) grounds, so as not to reward Plaintiffs' counsel's apparent gamesmanship.

reasons.

1. Plaintiffs Fail to Allege the Elements of a Section 631 Violation.

To state a claim under Section 631, Plaintiffs must plead facts showing that Noom used a "machine, instrument, or contrivance" to make an "unauthorized connection with any telegraph or telephone wire, line, cable, or instrument." Plaintiffs advance two theories of liability here: 1) that, through the "unauthorized connection," Noom obtained the contents of communications, or 2) that Noom "aids, agrees with, employs, or conspires" to allow FullStory to do so. Cal. Penal Code § 631(a). The Complaint fails to meet the statute's requirements under either theory.

a. Noom cannot wiretap its own communications.

To start, Noom cannot be held liable under Section 631 because it was a party to the purportedly intercepted "communications." California courts have long held that Section 631 applies "only to eavesdropping by a third party and not to recording by a participant to a conversation." *Membrila v. Receivables Performance Mgmt., LLC*, No. 09-cv-2790, 2010 WL 1407274, at *2 (S.D. Cal. Apr. 6, 2010) (citation omitted). For example, in *Rogers v. Ulrich*, the court explained that it cannot be "a secret to one party to a conversation that the other party is listening to the conversation; only a third party can listen secretly to a private conversation." 52 Cal. App. 3d 894, 899 (1975) ("'Eavesdropping' is the problem the Legislature meant to deal with; 'eavesdrop' is defined in Webster's 7th New Collegiate Dictionary (1972) as 'to listen secretly to what is said in private.'"). *See also Powell v. Union Pac. R.R. Co.*, 864 F. Supp. 2d 949, 955 (E.D. Cal. 2012) (granting a motion for summary judgment as to Section 631 claims against a first party "[g]iven the settled nature of the third-party focus of section 631").

Plaintiffs ignore this precedent and allege that Noom violated Section 631 by intercepting communications coming from visitors *to its own website*. (Compl. ¶ 62.) That theory is illogical and would effectively eviscerate the party exception under CIPA. It therefore must fail—just as it has when visitors to other websites have raised it under the Federal Wiretap Act. *See Cohen v. Casper Sleep, Inc.*, Nos. 17cv9325, 17cv9389, 17cv9391, 2018 WL 3392877, at *5 (S.D.N.Y. July 12, 2018) (dismissing with prejudice federal wiretap claims where the website owner was a party to the communication).

Plaintiffs may point to *Davis v. Facebook, Inc. (In re Facebook Inc. Internet Tracking Litig.)*, 956 F.3d 589, 599 (9th Cir. 2020), but that case is wholly inapposite because—unlike Noom—the defendant there was not the intended recipient of the intercepted communication. The Ninth Circuit grappled with a different question altogether: whether a third party (Facebook), could avail itself of the party exception when simultaneously intercepting GET requests *between an individual internet user and a third-party website*. *See generally In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589. In that case, Facebook installed "cookies [that] allegedly continued to capture information after a user logged out of Facebook and visited other websites." *Id.* at 596. Analogizing to similar cases involving defendants who were not the intended recipients of duplicated GET requests, the Court concluded that Facebook could not avail itself the party exception. *In re Facebook*, 956 F.3d at 607 (citing *United States v. Szymusckiewicz*, 622 F.3d 701 (7th Cir. 2010) (affirming conviction where defendant employed software that instructed employer's email to duplicate and forward all emails). Extending *Facebook* to hold that even intended recipients of internet communications (that is, user actions on the website that are tracked by that website) are not parties to those communications is facially implausible and contrary to both the plain language of that decision and well-established precedent.[3]

b. Noom cannot be liable for "aiding" or "conspiring" with a third party to listen to its own communications

Noom should not be held liable under any aiding and abetting theory of liability because it was a party to the communication with Plaintiffs. *See Powell*, 864 F. Supp. 2d at 954. In *Powell*, the court rejected Plaintiffs' argument that the participant to a call could be held liable for aiding and abetting pursuant to Section 631, reasoning that the statute "was aimed at one aspect of the privacy problem—eavesdropping, or the secret monitoring of conversations by third parties." *Id.* at 955 (citing *Ribas v. Clark*, 38 Cal. 3d 355, 359 (1985).). Reasoning that "[p]ublished cases are in accord that Section 631 only applies to third parties and not participants," it concluded that "[g]iven the settled nature of the third-party focus of section 631, the court declines to adopt

[3] Even to the extent there is any ambiguity as to *Facebook*'s application to this case (and there is not), "[s]ince we are dealing with a penal statute, language so ambiguous should be interpreted in favor of the alleged violator." *Warden v. Kahn*, 99 Cal. App. 3d 802, 817 n.3 (Ct. App. 1979).

plaintiff's alternative reading." *Id*. at 955-56 (citing *Rogers v. Ulrich*, 52 Cal. App. 3d 894, 898 (1975).)

Plaintiffs should find no solace in the recent *Revitch* decision, brought by the same Plaintiffs' counsel, in which the Court misapplied this case law and incorrectly denied dismissal of a claim against a first party to a communication for "enabling" wrongdoing by a third party. *Revitch v. New Moosejaw, LLC*, No. 18-cv-06827, 2019 WL5485330, at *2 (N.D. Cal. Oct. 23, 2019). This Court should decline to follow *Revitch*—which is not only an outlier, but fails to articulate a reasoned basis for its contravention of well-established precedent (its analysis spans a mere five sentences). To decide otherwise would radically alter the scope of California's eavesdropping law, and inundate California courts with a deluge of litigation—not unlike Plaintiffs' counsel's recent filing of over a dozen similar copycat lawsuits across California.

c. Any "communications" collected by FullStory were not "in transit."

Noom also could not have violated Section 631 under any theory because Plaintiffs do not specifically allege that Noom read any communications "in transit." *See Quigley v. Yelp, Inc.*, No. 17-cv-03771, 2018 WL 7204066, at *4 (N.D. Cal. Jan. 22, 2018) (holding that a party cannot be liable under section 631 if plaintiffs have "not alleged facts giving rise to an inference that his communications were intercepted while 'in transit'"); *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 878 (9th Cir. 2002) (holding that federal wiretap violations, a useful analog to CIPA, must allege "acquisition contemporaneous with transmission"); *cf. Cline v. Reetz-Laiolo*, 329 F. Supp. 3d 1000, 1050-51 (N.D. Cal. 2018) (CIPA's "in transit" element is analogous to the federal Wiretap Act's "intercepted" element and requires the same analysis). Reading or acquiring the contents of a communication either *before* or *after* that communication is transmitted, does not qualify. *See Rosenow v. Facebook, Inc.*, No. 19-cv-1297, 2020 WL 1984062, at *7 (S.D. Cal. Apr. 27, 2020) (granting motion to dismiss federal wiretap claim where allegations that communications were intercepted "in transit" were "conclusory").

While Plaintiffs allege that FullStory's code is integrated into its clients' application code and claim that the Session Replay technology records communications in "real time," they fail to

support that allegation with even a cursory statement describing how the code is deployed and whether it is triggered simultaneously with the user's communications. (Compl. ¶¶ 18, 24, 25.) Indeed, Plaintiffs' other allegations suggest that the code is *not* simultaneously triggered. (*Id.* ¶ 27 ("you'll *essentially* be riding along *in near real time* with the user . . . ." (emphasis added)).) Such bare allegations are insufficient to sustain Plaintiffs' pleading burden. *See In re Vizio Inc. Consumer Priv. Litig.*, 238 F. Supp. 3d 1204, 1228 (C.D. Cal. 2017) (dismissing federal wiretap claim because the "conclusory allegation that Vizio intercepted their electronic communications 'during transmission'" was only supported by "vague allegations about how Vizio's data collection occurs in real-time.") Accordingly, Plaintiffs have not plausibly alleged that Noom configured FullStory's Session Replay tool in a manner to allow for instantaneous transmission to Noom.

Plaintiffs' failure to clearly plead that the code is deployed simultaneously is fatal to their claims. As other courts have observed, the delay between when information about Noom's website visitors is collected and when it is transmitted to FullStory makes that transmission akin to the sharing of a record of the communication between the visitor and Noom, and thus outside the reach of Section 631. *See Quigley*, 2018 WL 7204066, at *4; *Konop*, 302 F.3d at 878; *Revitch*, 2019 WL 5485330, at *2 (noting that a first party website "would not have violated [Section 631] by creating a record of [a website visitor's] communications and then later transmitting that record to" a third party session replay service provider); *Bunnell v. Motion Picture Ass'n of Am.*, 567 F. Supp. 2d 1148, 1153–54 (C.D. Cal. 2007) (noting the Ninth Circuit's "narrow definition" of "intercept" for purposes of the Wiretap act). Further, Plaintiffs' conclusory allegation that the communications were intercepted in "real-time" does not make it so, and this allegation, without more, cannot withstand dismissal.

These cases are well-reasoned: Section 631 is an eavesdropping statute, and sharing a record is not eavesdropping. *See Rogers*, 52 Cal. App. 3d at 898; *Ribas v. Clark*, 38 Cal. 3d 355, 360 (1985) (explaining that section 631 only applies to direct interception of communications because "a substantial distinction has been recognized between the secondhand repetition of the contents of a conversation and its simultaneous dissemination to an unannounced second auditor"); *see also Hernandez v. Path, Inc.*, No. 12-CV-01515, 2012 WL 5194120, at *5 (N.D. Cal. Oct. 19,

2012) (dismissing Section 631 claims for, *inter alia*, failing to show "intercep[tion] [of] a communication in transit"); *Bradley v. Google, Inc.*, No. C 06-05289, 2006 WL 3798134, at *6 (N.D. Cal. Dec. 22, 2006) (plaintiff failed to state a CIPA claim because "she [did] not allege[ ] that Google intercepted her communications, only that her stored emails were deleted from her account").[4] For this reason as well, Plaintiffs' Section 631 claims fail and should be dismissed with prejudice.

2. Plaintiffs Fail to Allege Sufficient Facts to Support a Section 635 Claim.

Plaintiffs claim that Noom violated Section 635 because it "intentionally manufactured, assembled, sold, offered for sale, advertised for sale, possessed, transported, imported, and/or furnished a wiretap device that is primarily or exclusively designed or intended for eavesdropping upon the communication of another." (Compl. ¶ 72.) This claim should also be dismissed with prejudice for two independent reasons.

To start, Plaintiffs lack both constitutional and statutory standing to pursue a Section 635 claim because CIPA's private right of action cannot be extended to permit suits predicated on the mere "possession" of an alleged eavesdropping device. As to statutory standing, CIPA only grants a private right of action to "[a]ny person who has been injured by a violation of this chapter." Cal. Penal Code § 637.2(a). Likewise, to satisfy Article III standing, a plaintiff must allege "injury in fact," *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1547 (2016). To meet this standard, a plaintiff "must show that [she] . . . suffered an invasion of a legally protected interest that is concrete and particularized" from the alleged violation, and that the defendant's actions "affect[ed] the plaintiff in a personal and individual way." *Id.* (citation omitted).

Here, Plaintiffs do not meet either standard because they merely allege that Noom *possessed* a wiretap device (allegedly developed by FullStory) and a range of data that *could* be collected by FullStory's code. Plaintiffs make no allegation of injury from the alleged violation of Section 635, and possession of a device is not connected to any injury, real or imagined, and so cannot meet the

[4] *Ribas* is not to the contrary. 38 Cal. at 360. There, the Court held that a defendant's "listen[ing] on an extension telephone" to a live conversation was an interception of a communication in transit. *Id.* at 363. Unlike in this case, there was no basis to conclude there was any delay between the transmission of the message and the allegedly unlawful interception.

Spokeo standard.

In *Cohen*, for example, another case brought by the same Plaintiffs' counsel against a first-party website employing "session replay" tools, the court held that it would be "constitutionally problematic" to accord a private right of action for possession of a wiretap device such that "plaintiffs who suffered no injury in fact would still be able to sue." 2018 WL 3392877, at *5 (citation omitted). The same reasoning holds here. Allowing suit for mere possession of an eavesdropping device, without any allegation of injury, would obviate the need for Article III standing and raise serious constitutional concerns.

Noom acknowledges that the court in *Revitch* reached a different conclusion. 2019 WL 5485330, at *5. There, the court concluded without elaboration that Plaintiffs had sufficiently pled injury by parroting the statutory requirements and "alleg[ing] injuries traceable to Moosejaw's possession and use of the device." *Id.* at *3. In contrast to *Revitch*, Plaintiffs fail to allege any specific injury here. Instead, Plaintiffs in this case generally allege that "Defendants recorded Plaintiffs' electronic communications," (Compl. ¶ 2); they had a "reasonable expectation that their PII, PHI, and other data would remain confidential," (*id.* ¶ 80); and that "session recording technologies" such as FullStory's can leave users vulnerable to data leaks and the harm resulting therefrom. (*Id.* ¶ 29.) Plaintiffs also do not plead that Noom compiled this data in any fashion, correlated this data with their personal profiles, created any profile or sold the data to third parties. To the contrary, Plaintiffs allege that the tool "help[s] businesses improve their website design and customer experience." (*Id.* ¶ 17.) These facts are insufficient to demonstrate any concrete injury. *Cf. Cahen v. Toyota Motor Corp.*, 717 F. App'x 720, 724 (9th Cir. 2017) (holding that claims of unauthorized data sharing of non-individually identifiable driving history did not meet Article III standing requirements).

Even if *Revitch* was otherwise on-point, the court's decision is contrary to the plain language of the statute as well as the decisions of many other courts that have made clear that CIPA's federal analogue, the Wiretap Act, does not provide a private right of action for the manufacture, possession, and/or sale of wiretap devices. *See In re Lenovo Adware Litig.*, No. 15-md-2624, 2016 WL 6277245, at *7 (N.D. Cal. Oct. 27, 2016) ("Section 2512 [federal Section 635

analogue] however, does not establish a private right of action—it addresses only criminal liability."); *see also DirecTV, Inc. v. Treworgy*, 373 F.3d 1124, 1129 (11th Cir. 2004) (concluding that "the language of section 2520(a) does not create a private right of action against a person who possesses a device in violation of section 2512(1)(b)."). Accordingly, and consistent with these cases, this Court should dismiss Plaintiffs' Section 635 claim with prejudice.

Plaintiffs' Section 635 claim fails for another reason as well. Aside from their bare recital of the statute's requirements, Plaintiffs fail to allege sufficient facts to show the alleged "code" installed on Noom's website is a device "primarily or exclusively designed" for eavesdropping. In the absence of a statutory definition, courts "look to the plain meaning" of the disputed terms. *Friends of Yosemite Valley v. Norton*, 348 F.3d 789, 796 (9th Cir. 2003). Merriam-Webster defines eavesdropping as "the act of secretly listening to something private," an allegation conspicuously missing from Plaintiffs' complaint. *Eavesdropping*, Merriam-Webster, https://www.merriam-webster.com/dictionary/eavesdropping; (Compl. ¶¶ 72, 73.) As Plaintiffs note, the code simply collects data willingly typed onto Noom's website, much the same as "content from third-party servers" is collected through "analytics tools, advertising networks, code libraries and other utilities," which are "part of routine internet functionality." *In re Facebook Internet Tracking Litig.*, *supra*, 263 F. Supp. 3d 836, 846 (N.D. Cal. June 30, 2017) (overturned on other grounds); *cf. Low v. LinkedIn Corp.*, 900 F. Supp. 2d 1010, 1025 (N.D. Cal. 2012) (finding that LinkedIn did not commit a "highly offensive" invasion of users' privacy by disclosing users' browsing histories to third parties); *In re Google, Inc. Priv. Pol'y Litig.*, 58 F. Supp. 3d 968, 988 (N.D. Cal. 2014) (finding that Google's collection and disclosure of users' data, including their browsing histories, "do not plausibly rise to the level of intrusion necessary to establish an intrusion claim").

While Plaintiffs assert that FullStory's "code" is designed to collect non-confidential keystroke information, they do not explain why that function makes it a device "primarily or exclusively designed" for *eavesdropping*. (Compl. ¶¶ 72, 73.) Indeed, this code allegedly behaves and is used in a manner identical to any technology designed to facilitate web-browsing activity, including cookie technology, which can be used for a variety of purposes. *Cf.*, *In re DoubleClick, Inc. Priv. Litig.*, 154 F. Supp. 2d 497, 502-03 (S.D.N.Y. 2001) (explaining how cookies are

computer programs commonly used by websites to store useful information that help with website operation, just as session replay tools employ computer programs do as well). Given their failure to allege what communications this code intercepts, or how this code is exclusively for eavesdropping and therefore could be considered a device within the meaning of the statute, Plaintiffs have not stated a claim under Section 635 and this cause of action should be dismissed with prejudice.

B. Plaintiffs Fail to Allege an Invasion of Privacy under the California Constitution.

"The California Constitution and the common law both set a high bar for an invasion of privacy claim," *Belluomini v. Citigroup, Inc.*, No. CV 13-01743, 2013 WL 3855589, at *6 (N.D. Cal. July 24, 2013), and that bar has not been met here. The Supreme Court of California describes the necessary violation as one "so serious in nature, scope, and actual or potential impact as to constitute an egregious breach of the social norms." *Hernandez v. Hillsides, Inc.*, 47 Cal. 4th 272, 287 (2009) (internal quotation marks and citation omitted). Courts in this District have held that "[e]ven disclosure of personal information, including social security numbers, does not constitute an 'egregious breach of the social norms.'" *Low*, 900 F. Supp. 2d at 1025.

To plead a claim for invasion of privacy under the California Constitution, Plaintiffs must allege: "(1) a legally protected privacy interest; (2) a reasonable expectation of privacy under the circumstances; and (3) conduct by the defendant that amounts to a serious invasion of a protected privacy interest." *Moreno v. S.F. Bay Area Rapid Transit Dist.*, No. 17-cv-2911, 2017 WL 6387764, at *8 (N.D. Cal. Dec. 14, 2017); *see In re Yahoo Mail Litig.*, 7 F. Supp. 3d 1016, 1041 (N.D. Cal. 2014).

Applying these standards, Plaintiffs fail to explain how the browsing conduct on Noom's website is "*sensitive* and *confidential*." *In re Yahoo Mail Litig.*, 7 F. Supp. 3d at 1041 (internal quotation and citation omitted) (emphasis in the original) (finding that there is no legally protected privacy interest in the contents of emails generally, only in content that is sensitive and confidential). In fact, Plaintiffs fail to allege facts establishing any of these elements, much less all three, and therefore the Court should dismiss this claim with prejudice.

1. Plaintiffs Fail to Allege a Legally Protected Privacy Interest.

To withstand dismissal of an invasion of privacy claim, Plaintiffs must allege a legally protected privacy interest. *Hill v. Nat'l Collegiate Athletic Ass'n*, 7 Cal. 4th 1, 35 (1994). "Just as the right to privacy is not absolute, privacy interests do not encompass all conceivable assertions of individual rights." *Id.* Legally recognized privacy interests are generally categorized in two classes: (1) interests "in precluding the dissemination or misuse of *sensitive and confidential information* ('informational privacy');" and (2) interests in making intimate personal decisions or conducting personal activities without intrusion ("autonomy privacy"). *Id.* (emphasis added).

Although Plaintiffs parrot these legal requirements and generally allege that they have an interest in "precluding the dissemination and/or misuse" of their confidential information, and in making personal decisions and/or conducting personal activities without observation, (Compl. ¶ 78), they fail to plead facts to establish a legally protected informational privacy *or* autonomy privacy interest.

Autonomy privacy typically involves cases "alleging *bodily* autonomy" and courts generally do "not find sufficient cause to extend the bodily autonomy cases to data autonomy." *In re Google Location History Litig.*, 428 F. Supp. 3d 185, 198 (N.D. Cal. 2019) (emphasis in original); *In re Yahoo Mail Litig.*, 7 F. Supp. 3d at 1039 ("the Court construes Plaintiffs' claim as asserting only an informational privacy interest, as California courts have discussed autonomy privacy in the context of cases alleging *bodily* autonomy."). Since no bodily autonomy harm is alleged in the Complaint, Plaintiffs have failed to allege a legally protected privacy interest on this theory.

As to the informational privacy interest, Plaintiffs allege, albeit in a conclusory fashion, that Noom collected information during their use of Noom's website, such as their email address, IP address, location of the visit, height and weight, age range, and diet and exercise habits. (Compl. ¶ 41.) These allegations fail to state a claim for multiple reasons.

First, not all personally identifying information is subject to constitutional protection. "The disclosure of mere contact information, such as names and addresses, does not unduly interfere with one's right to privacy." *Cabral v. Supple, LLC*, No. EDCV 12-85, 2012 WL 12895825 (C.D.

Cal. Oct. 3, 2012). Similarly, "[a] person's general location is not the type of core value, informational privacy explicated in *Hill*." *Fredenburg v. City of Fremont*, 119 Cal. App. 4th 408, 423 (2004); *In re Google Location History Litig.*, 428 F. Supp. at 198. Indeed, even in the context of private *medical* information, courts have held that "[p]laintiffs and the [c]lass have no legally protected privacy interest in de-identified information . . . ." *London v. New Albertson's, Inc.*, No. 08-cv-1173, 2008 WL 4492642, at *8 (S.D. Cal. Sept. 30, 2008) (dismissing California Const. Art. I. Sec. 1 claim). As noted above, Plaintiffs do not allege this information—even if collected—is or can be linked to them in any fashion, and their claims fail for this reason.

Second, courts reject the application of information privacy claims where—as here—the defendants "only tracked and collected data during use of [defendant's] services." *In re Google Location History Litig.*, 428 F. Supp. 3d at 198.

Third, Plaintiffs do not plead, as they must, that the information they provided to Noom was "disseminate[d]" or "misuse[d]" in any fashion. *Hill*, 7 Cal. 4th at 35; *see also Orff v. City of Imperial*, No. 17-CV-0116 W (AGS), 2017 WL 5569843, at *9 (S.D. Cal. Nov. 17, 2017) (quoting *Hill* as requiring dissemination for an actionable common law invasion of privacy claim). Quite the opposite, Plaintiffs only allege that the information was used to "improve website design and customer experience." (Compl. ¶ 17.)

2. Plaintiffs Fail to Allege a Reasonable Expectation of Privacy.

Plaintiffs' privacy claim also fails because they do not plead that they had a reasonable expectation of privacy under the circumstances. "A 'reasonable' expectation of privacy is an objective entitlement founded on broadly based and widely accepted community norms." *Hill*, 7 Cal. 4th at 36. In determining whether an "objective entitlement" is present, "[c]ustoms, practices, and [the] physical settings surrounding particular activities" are taken into consideration, as are "*advance notice*" and "the presence or absence of opportunities to *consent voluntarily* to activities impacting privacy interests . . . ." *Id.* at 36-7 (emphasis added). Further, "[t]he plaintiff in an invasion of privacy action must have conducted himself or herself in a manner consistent with an actual expectation of privacy, i.e., he or she must not have manifested by his or her conduct a voluntary consent to the invasive actions of defendant." *In re Yahoo Mail Litig.*, 7 F. Supp. 3d at

1037–38 (internal citations omitted).

Here, Plaintiffs do not allege conduct consistent with an expectation of privacy: to the contrary, they claim that Noom monitored their browsing conduct on *Noom's website.* (Compl. ¶ 2 (stating that "[d]uring [Plaintiffs'] visits [to Noom's website], Defendants recorded Plaintiffs' electronic communications").) And while Plaintiffs generically contend that they "had a reasonable expectation that their PII, PHI, and other data would remain confidential," nowhere do Plaintiffs claim they had an actual expectation that their activity was or should be hidden *from Noom.* (*Id.* ¶ 80.) Even if they had advanced such an allegation, such an expectation would be patently unreasonable. Far from being hidden, their interactions with Noom's website were themselves intentional communications with Noom's servers. *See Cohen*, 2018 WL 3392877, at *3 (analyzing similar claims and finding "[i]t is clear that the Retailers were parties to the communications . . . .").

Moreover, virtually all consumer-facing websites track the conduct of web visitors for myriad reasons, including enhancing the browsing experience and site functionality—for example, any retailer must track which items are added to a digital shopping cart for that feature to function. Similarly, Noom relies on information that Noom users input on the site in order to improve those users' experience on the site and with its weight loss program. Given the near-universal practice of consumer-facing websites, no user can reasonably expect that the web pages she visits, or the information she provides to the operator of such a website, are hidden from that operator.

3. Plaintiffs Fail to Allege Noom's Conduct was a Serious Invasion of Privacy.

Even if Plaintiffs had a legally protectable and objectively reasonable expectation that no party could view their activity on Noom's website, Noom's alleged monitoring would still not be highly offensive or meet the "high bar" for a common law invasion of privacy claim. *See Low*, 900 F. Supp. 2d at 1025 (noting the high bar for such claims). To be a serious invasion of privacy requires the alleged conduct to be an egregious violation of social norms. *In re Yahoo Mail Litig.*, 7 F. Supp. 3d at 1042. Notably, courts have held that even the collection and subsequent dissemination of user data for marketing purposes is not a serious invasion of privacy. *See In re*

Google Inc. Priv. Pol'y Litig., 58 F. Supp. 3d 968, 985 (N.D. Cal 2014) (rejecting an invasion of privacy claim for collecting location information from users, associating it with other private user information, and then disclosing the commingled data to "third-party developers" in ways that allegedly violate the defendant's own policies). It cannot be, then, that the routine analysis of web activity for purposes of analyzing "website design and customer experience" passes this high bar. (Compl. ¶ 17.)

The California Court of Appeals' decision in *Folgelstrom v. Lamps Plus, Inc.* is instructive. There, plaintiff asserted claims based on the collection of personally identifiable information that was shared with third-party marketing firms for the purpose of marketing to potential customers. 195 Cal. App. 4th 986, 992 (2011). The court found "obtaining plaintiff's [information] without his knowledge or permission, and using it [for marketing purposes] . . . . is not an egregious breach of social norms, but routine commercial behavior." *Id*. The equally routine, less invasive, practice of using customer information for website functionality—and employing third-party companies to act as a proxy in said efforts—cannot therefore be an egregious violation of social norms that is highly offensive. Indeed, Noom's use of a third party to collect this information in an anonymized or pseudonymized manner is arguably *more* privacy protective, as it limits the ability of Noom or its third-party vendor to deanonymize or create individual profiles from these data directly.

The Court's reasoning in *Folgestrom* is consistent with a large body of case law in this district that finds even the allegedly surreptitious collection and dissemination of personally identifiably information, such as unique device identifiers, browsing activity, and address information, for commercial purposes, is not enough to meet the exacting "highly offensive" standard. *See, e.g.*, *In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1063 (N.D. Cal. 2012) (dismissing with allegations that defendants disclosed to third parties "the unique device identifier number, personal data, and geolocation information from Plaintiffs' iDevices."); *Yunker v. Pandora Media, Inc.*, No. 11-CV-03113, 2013 WL 1282980, at *14-15 (N.D. Cal. Mar. 26, 2013) (same with allegations of "obtain[ing] [plaintiff's] PII and provided that information to advertising libraries for marketing purposes, in violation of the terms of Pandora's Privacy Policy."); *In re Google Android Consumer Priv. Litig.*, No. 11-MD-02264, 2013 WL 1283236, at *2, *9-11 (N.D.

Cal. Mar. 26, 2013) (same with allegations of tracking and sharing of "highly detailed and confidential [PII] over a substantial period of time without [Plaintiffs'] knowledge or consent"). Indeed, even negligent conduct that leads to theft of highly personal information, such as social security numbers, does not "approach [the] standard" of actionable conduct under the California Constitution and thus does not constitute a violation of Plaintiffs' right to privacy. *See Ruiz v. Gap, Inc.*, 540 F. Supp. 2d 1121, 1127–28 (N.D. Cal. 2008) *aff'd*, 380 F. App'x 689 (9th Cir.2010).

Neither *Facebook* nor *Revitch* is to the contrary. In *Facebook*, the Court held that the plaintiffs plausibly alleged an invasion of privacy based on allegations that the defendant created a comprehensive "cradle-to-grave profile" that "constantly compiled and updated its database with the users' browsing activities." *In re Facebook Internet Tracking Litig.*, 956 F.3d at 599. According to that court, the plaintiffs identified sufficient facts to survive a motion dismiss based on "surreptitious data collection *when individuals were not using Facebook*" and their allegations that "internal Facebook communications reveal that the company's own officials recognized these practices as a problematic privacy issue." *Id.* at 606 (emphasis added). No such allegations are pled here, and any effort to contort that case to fit the facts alleged in the Complaint—i.e., electronic communications directly between a website user and its own visitors—would be contrary to well-settled authority cited above.

Meanwhile in *Revitch*, the court relied on allegations that the code in question "scanned [plaintiff's] computer for files that revealed his identity and browsing habits." *Revitch*, 2019 WL 5485330, at *3. Those facts are not pled in this case. As explained above, the routine collection of information provided to a first party website and its vendor cannot possibly satisfy the strict standard for invasion of privacy claims under the California Constitution. Accordingly, neither *Facebook* nor *Revitch* saves Plaintiffs' invasion of privacy claims, and they too must be dismissed.

VI. CONCLUSION

For the reasons above, this Court should grant the Motion and dismiss the case in its entirety, with prejudice.

Dated: December 11, 2020

COOLEY LLP
MICHAEL G. RHODES (116127)
KYLE C. WONG (224021)
AARTI REDDY (274889)
CHARLES A. WOOD (310702)

/s/ Michael G. Rhodes
Michael G. Rhodes
Attorneys for Defendant
NOOM, INC